IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	**Case No. CR-16-119-R**
	)	
CHAD NATHAN HUDSON, *et al.*,	)	
	)	
Defendants.	)	

ORDER

Before the Court are Defendants' Motions to Suppress evidence from Title III wiretaps authorized on June 17th, 2016, for Defendant Coker's cellphone ("TT1"[1]) and on July 1st, 2016, for Defendant Brown's cellphone ("TT2"), Docs. 1124, 1125, 1133, 1134. *See* Orders Authorizing Interception, Docs. 1191-2 (TT1) and 1191-4 (TT2).[2] Defendants Brown and Potts move to suppress TT1 and TT2 intercepts because they were allegedly outside the territorial jurisdiction of the Western District of Oklahoma; they also challenge content allegedly intercepted from TT1 before that wiretap was authorized. *See* 18 U.S.C. § 2518(3), (10)(a)(ii)–(iii); Docs. 1133, 1134. Additionally, Defendants Yargee, Brown, and Potts challenge the sufficiency of the TT1 and TT2 wiretap applications in complying with Title III's necessity requirement—inclusion of "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they

[1] "TT1" and "TT2" refer to "Target Telephone 1" and "Target Telephone 2."
[2] *See also* Docs. 1139 (Granting Defendant Brown joinder of Defendant Yargee's motions, Docs. 1124 and 1125); 1266 (Granting Defendant Potts joinder of Defendant Yargee's motions, Docs. 1124 and 1125).

reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. § 2518(1)(c); *see* 18 U.S.C. § 2518(10)(a)(ii); Docs. 1124 and 1125. The Court finds that the Government made a sufficient necessity showing, obtained valid authorization orders, and conducted wiretaps in conformity with those orders. Accordingly, the Court denies Defendants' Motions for the following reasons.

I. Background

Defendants Brown, Potts, and Yargee are charged with conspiracy to possess and distribute methamphetamine and heroin and various other crimes related to the Irish Mob gang's alleged drug-trafficking operation. *See* Second Superseding Indictment, Doc. 601. According to the Indictment, Mob leaders incarcerated in an Oklahoma state prison, including Defendants Brown and Potts, used contraband cellphones to direct suppliers, couriers, and distributors to move cash, methamphetamine, and heroin between various stash houses around the Oklahoma City area; Defendant Yargee was allegedly one of these couriers. *See id.* at 3–8.

Defendants Brown, Potts, and Yargee challenge the sufficiency of two wiretap orders and seek to suppress any resulting incriminating content. On June 17, 2016, Chief United States District Judge for the Western District of Oklahoma, Joe Heaton, authorized the TT1 wiretap of Richard Coker's cellphone while he was incarcerated in McAlester State Penitentiary in the Eastern District of Oklahoma.[3] *See* Doc. 1192. The order relied on FBI Special Agent ("SA") Jamie Walker's affidavit, which described the Government's

[3] The Court sentenced Defendant Coker on December 5, 2017, to 30 years imprisonment for his role in the conspiracy. *See* Docs. 1237 and 1238.

investigation until that point and why traditional non-wiretap investigative techniques were unlikely to uncover the conspiracy's full scope. *See* Doc. 1191-1. Then on July 1, 2016, U.S. District Judge for the Western District of Oklahoma, Timothy DeGiusti, ordered the TT2 wiretap of Defendant Brown's cellphone, relying on another affidavit by SA Walker that similarly outlined the investigation and necessity for a wiretap. *See* Docs. 1191-3; 1191-4.

II. Standing and Applicability of Title III

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, codified at 18 U.S.C. §§ 2510–22, "generally forbids the intentional interception of wire communications, such as telephone calls, when done without court-ordered authorization.'" *United States v. Faulkner*, 439 F.3d 1221, 1223 (10th Cir. 2006) (quoting *United States v. Workman*, 80 F.3d 688, 692 (2d Cir. 1996)). Communications intercepted in violation of Title III are subject to suppression, 18 U.S.C. § 2515, but only an "aggrieved person" has standing to move for suppression. *Id.* § 2518(10)(a); *see Faulkner*, 439 F.3d at 1223. An "'aggrieved person' means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed." *Id.* § 2510(11). Moreover, "[a] defendant bears the burden of proving that a wiretap is invalid once it has been authorized." *United States v. Ramirez-Encarnacion*, 291 F.3d 1219, 1222 (10th Cir. 2002)

Defendant Yargee is not an aggrieved person with standing to move for suppression of intercepted TT1 content. *Id.* He makes a conclusory assertion otherwise, Doc. 1125, at 2–3, but the Government notes that it only directed the TT1 wiretap at Richard Coker and

Gary Schneider; Yargee also fails to show a TT1 intercept to which he was a party. *See id.*; Doc. 1191-2, at 1. Nonetheless, the Government concedes that Brown and Potts are aggrieved persons with respect to TT1 intercepts and that Brown, Potts, and Yargee are aggrieved persons with respect to TT2 intercepts. *See United States v. Dewitt*, 946 F.2d 1497, 1499–1500 (10th Cir. 1991) ("[T]he government has waived this [standing] issue by failing to raise it below.").

The Government makes two arguments that despite maintaining standing to challenge one or both wiretap authorization orders, Defendants are not entitled to Title III protection of communications through a contraband cellphone in prison.[4] First, Title III excludes instances where "a person acting under color of law . . . intercept[s] a wire . . . communication" and "one of the parties to the communication has given prior consent to such interceptions." 18 U.S.C. § 2511(2)(c). The Government argues that Oklahoma state prisoners implicitly consent to wiretap interception. *See* Doc. 1191, at 8–10. In the context of prison-run telephones, the question is settled. *See United States v. Verdin-Garcia*, 516 F.3d 884, 895 (10th Cir. 2008) ("[W]e agree with the other circuits having considered the question that where the warnings given and other circumstances establish the prisoner's awareness of the possibility of monitoring or recording, his decision to take advantage of that [telephone] privilege implies consent to the conditions placed upon it."). Defendants' consent is implied from repeated warnings regarding phone-monitoring in the

[4] The Government argues that it requested Court authorization under Title III as a precautionary measure, even though it believes Defendants are exempt from Title III protection. *See* Doc. 1191, at 7. Defendants seek to use these wiretap applications as evidence that the Government argues for this implied exception in bad faith. *See* Doc. 1256, at 4. The Court declines to make any such implication for the Government proceeding with caution.

Oklahoma Department of Corrections' ("ODOC") Offender Orientation Manual and Policy Statement distributed to inmates like Brown and Potts upon arrival. *See* Docs. 1191-5; 1191-6.

However, the ODOC documents' repeated references to monitoring by "facility staff officials" of "general telephone calls" clarifies that Defendants Brown and Potts' implied consent to monitoring was limited to prison-run telephones, not to contraband cellphones. *Id.* Otherwise, why would inmates allegedly use contraband cellphones to conduct drug-trafficking business, if not to evade monitoring by prison staff? The Government fails to show how consent in one context necessarily supplies consent in another.

Second, the Government argues that even if the Court declines to find consent as prescribed by the statute, there is an implicit Title III exception for intercepts involving contraband cellphones. Title III "protects an individual from all forms of wiretapping except when the statute specifically provides otherwise." *Faulkner*, 439 F.3d at 1223 (quoting *United States v. Hammond*, 286 F.3d 189, 192 (4th Cir. 2002)). The statute also explicitly lists various exceptions at 18 U.S.C. § 2511(2), none of which directly speak to this issue. Because the Government makes a proper showing of territorial jurisdiction and wiretap necessity below, the Court assumes for purposes of the Motions that Title III applies and does not reach the contraband exception issue. *But see United States v. Ballesteros*, No. 13-CR-4514-BEN, 2015 WL 468373, at *4 (S.D. Cal. Feb. 3, 2015).

III. Territorial Jurisdiction

Defendants Brown and Potts argue that the TT1 and TT2 wiretaps were facially insufficient because Chief Judge Heaton and Judge DeGiusti lacked territorial jurisdiction over the intercepts. *See* 18 U.S.C. § 2518(3), (10)(ii); Doc. 1133. An "'intercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4). An authorizing court has jurisdiction where Title III interception occurs—"both where the tapped telephones are located and where law enforcement officers put their listening post." *United States v. Dahda*, 853 F.3d 1101, 1112 (10th Cir.), *cert. granted on other grounds*, 138 S. Ct. 356 (2017); *see also United States v. Tavarez*, 40 F.3d 1136, 1138 & n.2 (10th Cir. 1994) (finding the same definition of "interception" in the "Oklahoma counterpart to Title III," *Dahda*, 853 F.3d at 1112, the Oklahoma Security of Communications Act). Because interception occurs in both places, the Government can show proper territorial jurisdiction by merely satisfying one of the two requirements. *See id.*

It is undisputed that the Government targeted TT1 and TT2 cellphones located in the Eastern District of Oklahoma, outside the authorizing jurisdiction. However, Chief Judge Heaton and Judge DeGiusti ordered that "all interceptions conducted" on TT1 and TT2 must be at the FBI's Oklahoma City office within the Western District of Oklahoma. Docs. 1191-2, at 7; 1191-4, at 6–7. In other words, the "listening posts" were in the Western District and both judges had jurisdiction to order the wiretaps.[5] *Dahda*, 853 F.3d at 1112.

[5] Defendants incorrectly argue that AT&T contractors in Florida were the first to intercept TT1 and TT2 communications because they "technical[ly] transfer[ed] . . . the content of the calls" to the Government.

Defendants argue that the Court should ignore *Dahda*'s "listening post" holding because the Supreme Court granted certiorari and the opinion's logic is unsound; however, both *Dahda* and *Tavarez* are binding precedent and every circuit to consider this question has adopted the same territorial jurisdiction definition. *Id.* The only remaining question for the Supreme Court concerns whether Title III requires suppression when an authorizing court exceeds its territorial jurisdiction. *See* Brief for Petitioner at I, *Dahda v. United States* (No. 17-43), 2017 WL 5952676. That issue is plainly not before the Court. Chief Judge Heaton and Judge DeGiusti properly ordered TT1 and TT2 interception in the Western District of Oklahoma, "where law enforcement officers put their listening post," and Defendants fail to demonstrate that the Government strayed from these orders. *Dahda*, 853 F.3d at 1112; *see Ramirez-Encarnacion*, 291 F.3d at 1222 ("A defendant bears the burden of proving that a wiretap is invalid once it has been authorized.").

IV. Necessity

The Court next turns to the substance of the TT1 and TT2 wiretap applications. Title III requires that the Government's wiretap application include "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. § 2518(1)(c). The authorizing court subsequently reviews the application to

Doc. 1256, at 12; *see also* Doc. 1258 at 4–5. *Dahda* and *Tavarez* make clear that the relevant jurisdictional inquiry into an intercept's location is "where law enforcement officers put their listening post" and "where the communication is [first] heard." Therefore, any further inquiry into how AT&T facilitates the Government's interception is unnecessary. *United States v. Dahda*, 853 F.3d 1101, 1112 (10th Cir.), *cert. granted on other grounds*, 138 S. Ct. 356 (2017); *see also United States v. Tavarez*, 40 F.3d 1136, 1138 n.2 (10th Cir. 1994).

determine whether "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." *Id.* § 2518(3)(c). Now upon Defendants' suppression motion, the Court "examine[s] de novo whether 'a full and complete statement' was submitted meeting Section 2518(1)(c)'s requirements" and "reviews the conclusion that the wiretap[] [was] necessary in each situation for an abuse of discretion." *Ramirez-Encarnacion*, 291 F.3d at 1222 & n.2 (quoting *United States v. Armendariz*, 922 F.2d 602, 608 (10th Cir. 1990)).

It is unclear whether Defendants challenge both the sufficiency of the Government's necessity showing and the authorizing judges' ultimate findings. *See* Affidavits in Support of Application, Docs. 1191-1 (TT1) and 1191-3 (TT2); Orders Authorizing Interception, Docs. 1191-2 (TT1) and 1191-4 (TT2). Regardless, neither claim has merit, nor is suppression of the Government's intercepts warranted.

Defendants' arguments targeting the Government's Section 2518(1)(c) necessity showing are threefold. They claim that (1) previous law enforcement techniques were highly successful in uncovering the Irish Mob conspiracy—the wiretap application affidavits merely said "we want more," Doc. 1125, at 10; (2) the affidavits used boilerplate, unsubstantiated language to dismiss traditional techniques; and (3) the Government improperly "bootstrapped" by relying on the TT1 affidavit and failing to make an independent showing that the TT2 wiretap was necessary. Doc. 1124, at 5–6.

Title III's "necessity" requirement "guarantee[s] that wiretapping or bugging occurs only when there is a genuine need for it and only to the extent that it is needed." *Dalia v. United States*, 441 U.S. 238, 250 (1979). To satisfy necessity, the Government "must

explain with particularity" why each of the following traditional law enforcement techniques are insufficient to achieve the investigation's goals or are too dangerous:

> (1) standard visual and aural surveillance; (2) questioning and interrogation of witnesses or participants (including the use of grand juries and the grant of immunity if necessary); (3) use of search warrants; . . . (4) infiltration of conspiratorial groups by undercover agents or informants[; and (5) use of] pen registers or trap and trace devices . . . .

United States v. Castillo-Garcia, 117 F.3d 1179, 1187–88 (10th Cir. 1997*)*, *overruled on other grounds by Ramirez-Encarnacion*, 291 F.3d 1219. "[G]eneralities, or statements in the conclusory language of the statute, are insufficient to support a wiretap application." *Id.* at 1188.

However, just because the Government has exhibited some success with traditional techniques does not mean a wiretap is inappropriate. *See, e.g., United States v. Mandell*, 833 F.3d 816, 821–23 (7th Cir. 2016); *United States v. McGuire*, 307 F.3d 1192, 1198 (9th Cir. 2002) ("That there has been an indictment does not mean that a wiretap cannot gain evidence to make a prosecution more effective"); 1 James G. Carr *et al.*, *The Law of Electronic Surveillance*, § 4:39 at 414 (Thomson Reuters, Feb. ed. 2017) ("Where a large conspiracy is the target of the surveillance, the fact that conventional methods have developed enough evidence to indict or even convict some of its members does not preclude a finding of necessity"). In other words, Title III "necessity" is not an "exhaustion" requirement. *Castillo-Garcia*, 117 F.3d at 1187 (10th Cir. 1997). It merely requires that the Government prove it considered or attempted, in light of "the unique circumstances of [the] investigation," all "reasonable" investigatory methods. *Id.* at 1188.

The Court has considered SA Walker's affidavits supporting the TT1 and TT2 wiretaps independent of one another and in light of Defendants' arguments. Each affidavit includes a thorough and particularized discussion of why traditional law enforcement techniques were insufficient to accomplish the goals of this investigation. The TT1 wiretap's goal was "to identify all persons involved in this illegal activity and gather evidence sufficient to successfully prosecute each of these individuals, particularly **COKER** and his source(s) of supply of methamphetamine and heroin." Doc. 1191-1, at 31. The TT2 wiretap's goal was the same, only aiming particularly to identify "**BROWN** and his source(s) of supply of methamphetamine and heroin." Doc. 1191-3, at 19. In showing why a wiretap was necessary to accomplish these goals, SA Walker discussed the following techniques, each tailored to the respective TT1 and TT2 targets.

The affidavits first discussed the progress of the Government's confidential informants. The Government arranged various controlled purchases of methamphetamine and heroin to learn how their TT2 target, Brown, distributed drugs. *See* Doc. 1191-3, at 20–21. However, the Irish Mob, like other larger-scale drug-trafficking organizations, was "secretive and compartmentalized in such a way that persons within an enterprise do not know all the other members . . . and their respective roles, thereby insulating the enterprise in the event that an organization's member cooperates with law enforcement." *Id.* at 32. For example, one informant had been friends with Coker for over ten years, but Coker was still highly cautious of revealing anything about the Mob's day-to-day operations and the identities of his associates. *Id.* at 32–33. SA Walker also demonstrated how Defendant Brown was equally cautious and would not reveal his sources of supply. *See* Doc. 1191-3,

at 20–21. Further, any aggressive questioning of Coker or Brown from an informant would likely alarm them and undermine the investigation. Therefore, calling on SA Walker's experience with drug-trafficking investigations and his particular knowledge of the Irish Mob, the Government had reasons to believe its confidential informants could not help locate unknown coconspirators and stash houses.

Second, the affidavits demonstrated that physical surveillance was of limited value if not conducted in conjunction with other techniques such as wiretaps. The Government surveilled several controlled purchases orchestrated by Coker and Brown, but agents were unable to glean the full picture of the Irish Mob's operation. The Mob's drug couriers often lived out of hotel rooms, used vehicles registered to third parties, and took steps to elude surveillance. Further, surveillance of Coker and Brown at McAlester State Penitentiary—in "'The Walls,' where prisoners are kept in their cells 23 hours a day"—was severely frustrated because they were able to conduct business in-cell freely with the alleged protection of bribed prison guards. Docs. 1191-1, at 35–36; 1191-3, at 24–25.

Next, the Government declined to use undercover officers. It elaborated in its applications that Coker and Brown were unlikely to work with or trust unknown individuals any more than they would the Government's existing confidential informants—that is to say, if informants were insufficient to achieve the investigation's goals, so were undercover officers. Docs. 1191-1, at 36–37; 1191-3, at 25–27. There is also an inherent dangerousness in sending an undercover officer to buy drugs from a violent drug-trafficking operation. *Id.* SA Walker justified these assumptions with concrete evidence of Coker and Brown's paranoia regarding undercover law enforcement and of Coker's penchant for violence. *Id.*

SA Walker then discussed that while law enforcement had probable cause to obtain various search warrants, that approach would be premature. Agents executed one search warrant on a courier's house that yielded some evidence. *See* Doc. 1191-1, at 38. It evinced that the Government had yet to uncover several key stash houses and players in the Irish Mob. Therefore, executing search warrants would all but preclude "law enforcement's ability to single-handedly seize all drugs, drug proceeds, and assets being utilized by the enterprise." *Id.* Law enforcement also placed a tracker on a vehicle allegedly user by one major supplier, but that tracking data lacked context without round-the-clock surveillance and TT2 wire interception. *See* Docs. 1191-3, at 27.

The affidavits also dismissed financial investigation as a viable path. *See* Docs. 1191-1, at 40; 1191-3, at 30. The Government attested that the Irish Mob was largely a cash-based enterprise that took great lengths to hide any traces of their dealings.

SA Walker's affidavits also delineated various pen registers and caller identification devices that the Government employed to investigate TT1, TT2, and other cellphones. *See* Docs. 1191-1, at 40–42; 1191-3, at 30–32. This tactic was relatively successful to establish various associations between coconspirators. Without a wiretap, however, the Government could not identify the roles and level of participation of the call participants. Nor did the pen registers help identify which telephones were used by Coker's and Brown's sources of supply. This is because pen registers lack information on the actual parties to calls and the substance of conversations. Making matters more complicated, the targets of the Government's TT1 and TT2 wiretap applications often switched phones, used fictitious or

incomplete subscriber information,[6] and employed three-way calling, which creates a "confusing web of telephone calls that are difficult to decipher, particularly when even more callers are added." Doc. 1191-3, at 31.

Additionally, law enforcement declined to employ seizures of targets' garbage or cellphones or use of the grand jury. Docs. 1191-1, at 42–47; 1191-3, at 33–41. SA Walker represented that subjects of drug trafficking on this scale rarely leave behind potential evidence in their garbage, not to mention the additional logistical obstacle—McAlester State Penitentiary does not separate garbage by inmate, so identifying potential evidentiary material would be highly impractical. Law enforcement also faced the difficulty of Coker and Brown's alleged bribery of McAlester correctional officers and the fear of alerting targets to the investigation; each led the Government to believe that Coker and Brown would be able to continue operating their conspiracy without the seized cellphones "within a matter of days, if not hours." Docs. 1191-1, at 46; 1191-3, at 41. Moreover, SA Walker believed that subpoenaing Coker, Brown, or their associates to testify in front of a grand jury would be fruitless and counter-productive at that stage in the investigation. *See* Docs. 1191-1, at 43–44; 1191-3, at 35.

Lastly, SA Walker showed that arrests and testimonial cooperation were insufficient to accomplish the Irish Mob investigation's goals. Coker and Brown both allegedly orchestrated a drug-trafficking operation from prison—merely arresting them would not

[6] For example, the subscriber for TT1 was a "Prepaid Customer" with an address of "123 Your Street, Your Town," and the subscriber name for TT2 was "Cody Jones" from "12345 Gophone Way." Docs. 1191-1, at 41; 1191-3, at 32.

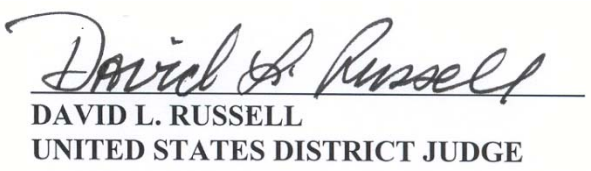
cripple the organization without first locating all stash houses and suppliers. *See* Docs. 1191-1, at 44; 1191-3, at 35–36. Law enforcement also had reasons to believe that full cooperation from defendants at that point was unlikely given other alleged co-conspirators' refusal to cooperate. More importantly, fear of retaliation was widespread. The affidavits listed various examples of violent witness intimidation and bribery in cases that implicated the Irish Mob. *See* Docs. 1191-1, at 45–46; 1191-3, at 37–38. Even if the Government chose to make more arrests before the wiretap applications and secured cooperation of some defendants, it believed that testimony was unlikely to dismantle the conspiracy.

In light of the Government's showing, Chief Judge Heaton and Judge DiGuisti acted well within their discretion in issuing the TT1 and TT2 wiretaps. SA Walker's lengthy affidavits confirmed that the Government used a range of law enforcement techniques insufficient to achieve the investigation's goals, and it declined to employ others for well-articulated, tailored reasons. This is a significant conspiracy case allegedly orchestrated from inside a state penitentiary. As a result, the authorizing judges found it necessary to employ wiretaps to uncover the full scope of wrongful conduct. Defendants have not met their burden of proving that the TT1 and TT2 wiretaps were invalid, and the Court defers to the judges' discretion in authorizing them. *See Ramirez-Encarnacion*, 291 F.3d at 1222.

Defendants Brown and Potts also make one last argument that the Government illegally initiated its TT1 wiretap before Chief Judge Heaton's authorization. In response, the Government provided sworn affidavits from the FBI and AT&T, the service provider for TT1, to dispel this notion. *See* Docs. 1191-7; 1191-8. The Court gave Defendants an opportunity to rebut this evidence in a hearing, which they failed to do.

Accordingly, the Court is satisfied that the Government demonstrated necessity for wiretaps, obtained valid authorization orders, and conducted the TT1 and TT2 wiretaps in conformity with those orders. The Motions to Suppress, Docs. 1124, 1125, 1133, and 1134, are DENIED.

IT IS SO ORDERED this 12th day of January, 2018.



DAVID L. RUSSELL
UNITED STATES DISTRICT JUDGE